UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/381,996	09/27/1999	MASAZUMI YAMADA	MTS-V03175	4678

7590 08/23/2006

RATNER & PRESTIA
ONE WESTLAKES BERWYN
SUITE 301 PO BOX 980
VALLEY FORGE, PA 194820980

EXAMINER	
CHEN, SHIN HON	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/381,996	YAMADA ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-28,30-45,47-49,53-57,59,63-65,68 and 69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4-28, 30-45, 47-49, 53-57, 59, 63-65, 68, and 69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 4-28, 30-45, 47-49, 53-57, 59, 63-65, 68, and 69 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 4-6, 22-26, 28, and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto et al. U.S. Pat. No. 5796828 in view of Kori U.S. Pub. No. 20010053979 (hereinafter Kori) and further in view of Aizawa U.S. Pat. No. 5646993 (hereinafter Aizawa)

As per claim 4, Tsukamoto teaches a data recording/reproducing system comprising a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data (Tsukamoto: column 4 lines 4-9: encipherer is coupled to descrambler to encrypt descrambled video signals to produce encrypted video signals; column 3 line 62: descrambler is coupled to tuner; column 3 line 51: tuner receives input digital signals), a recording means for recording said encrypted digital data and said encrypted contents key on a recording medium, a reproducing means for reproducing said encrypted digital data from said recording medium (Tsukamoto: column 4 lines 19-25: records video signal from encrypting means), and a decrypting means for decrypting said encrypted digital data

(Tsukamoto: column 4 lines 29-32: decrypt encrypted signals according to an encryption key). Tsukamoto does not explicitly teach key-encrypting key method for the encryption key and method for decrypting the encrypting key to decrypt the data. However, Kori teaches the method of encrypting contents key to generate an encrypted contents key to encrypt digital data (Kori: page 5 paragraph 79: A/V data is encrypted with key kd, and kd is encrypted corresponding to a predetermined key), and decrypting said encrypted contents key to restore said contents key, and a contents decrypting means for decrypting said encrypted digital data by using said contents key to obtain said digital data (Kori: page 5 paragraph 82: decrypt the key kd and then use kd to decrypt the A/V data), and wherein said encrypted contents key is recorded in a data area on said recording medium, from which data is not output outside (Kori:[0080]-[0081]: the data key is stored in header portion of the data). The key encrypting/decrypting method and contents encrypting/decrypting method can be carried out by the decipherer and encipherer within Tsukamoto's system or it can be carried out by adding separate encrypting/decrypting means for encrypting/decrypting said contents key as well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teaching of Kori within the system of Tsukamoto because using encrypted contents key would allow the system to be dual encrypted and it would take cryptanalysts more time and more a lot more effort to break the system if possible.

Furthermore, Tsukamoto teaches the method of erasing the video program on a certain date wherein the predetermined condition is satisfied if the key-encrypting key was stored on a previous date that is less than a specific number of days from a current date, or if a number of reproductions of the digital data is less than a specific number of reproduction (Tsukamoto:

column 9 lines 1-18 and column 9 line 64 – column 10 line 8). Tsukamoto does not explicitly teach the method of deleting only the key-encrypting key if key-encrypting key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the key-encrypting key at the time the A/V data is transmitted (Kori: [0081] and [0083]: transmitting the user management key to restrict the user to use the A/V data). Although Kori does not explicitly disclose only deleting the decryption key to render the content useless, Aizawa discloses deleting only the content encryption key to prohibit decryption of data (Aizawa: column 5 lines 46-55). It would have been obvious to one having ordinary skill in the art to erase only the key-encrypting key because the user management key ku is used is used to restrict access to the programming and by deleting the user management key, the encrypted video programming is rendered useless. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it restricts the user to use the A/V data without the presence of the user management key.

As per claim 5, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. Tsukamoto further teaches all of said means are provided for an integrated apparatus (Tsukamoto: column 3 lines 42-50: the receiving system).

As per claim 6, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. Tsukamoto further teaches said receiving means, said contents encrypting means and said contents decrypting means are provided for a tuner apparatus (Tsukamoto: column 3 line 50: tuner receives signal; column 3 line 62: descrambler coupled to tuner; column 4 line 4: encipherer coupled to descrambler), and said recording means and said reproducing means are provided for a VTR apparatus (Tsukamoto: column 4 lines 24-25:

recording/reproducing device, VTR). The receiving system disclosed by Tsukamoto can be referred to as the tuner apparatus since it contains a tuner and other components.

As per claim 22 and 23, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 6. Tsukamoto further teaches said tuner apparatus generates and stores billing information at the time of recording by said recording medium (Tsukamoto: column 6 lines 27-46: the user can pay to get full access to record or reproduce a video program; column 6 lines 60-64: the recorded video can be reproduced upon payment; figure 7a: the signal sent from the access control include purchase information). The signal sent from the access control implies that the billing information has been stored and generated within the tuner apparatus.

As per claim 24, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 23. Tsukamoto further discloses wherein information required to generate said billing information is recorded on said recording medium at the time of recording by said recording means, and said billing information is generated by using said required information at the time of reproduction by said recording means (Tsukamoto: figure 7A and column 15 lines 9-50: determine the access control signal corresponding to the selected video program).

As per claim 25, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 23. Tsukamoto further teaches the billing information is provided with limitation of the reproduction period of said recording medium (Tsukamoto: column 7 lines 50-51: reproduction is allowed until a certain date; column 7 lines 66-67: reproduction is allowed until certain time).

As per claim 26, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 23. Tsukamoto further teaches the billing information is provided with

limitation of the number of reproductions of said recording medium (Tsukamoto: column 7 lines 20-21: a video program can be reproduced for a certain number of times).

As per claim 28, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 22. Tsukamoto further teaches said tuner apparatus outputs said billing information to a service provider via communications (Tsukamoto: column 6 lines 27-46: broadcasting station communicates signals through communication link and modem; figure 6: connection to a broadcasting station).

As per claim 69, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. Tsukamoto further discloses a billing generator means for generating further billing of said digital data responsive to decryption of encrypted digital data using said changed contents key to obtain said digital data (Tsukamoto: column 9 lines 10-18).

4. Claims 7-10, 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori as applied to claim 4 above, and further in view of Fox et al. U.S. Pat. No. 5790677 (hereinafter Fox).

As per claim 7, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. Tsukamoto-Kori does not explicitly teach the method of using public key to encrypt contents key and decrypt encrypted contents key by using a secret key. However, Fox teaches said second encrypting is carried out by using a public key, and said encrypted contents key is decrypted by using a secret key corresponding to said public key (Fox: column 2 lines 62-67: encrypt key with a public key and decrypt the key with private key that matches the public encryption key). It would have been obvious for one having ordinary skill in the art at the

time of applicant's invention to combine the teachings of Tsukamoto, Kori, and Fox because the dual encryption allows stronger security by using strong asymmetric key pair while encrypting large amount of data using more efficient symmetric key.

As per claim 8, Tsukamoto further teaches a data recording/reproducing system in accordance with claim 7, wherein said key decrypting means is provided for said tuner apparatus (Tsukamoto: Figure 2: the decipherer is included in the receiving system). The receiving system can be described as the tuner apparatus for which a tuner is included in the system along with several other components.

As per claim 9, Tsukamoto further teaches a data recording/reproducing system in accordance with claim 8, wherein said public key and said secret key are keys inherent in said tuner apparatus (Tsukamoto: column 4 lines 12-15: the encryption key is prestored in encipherer; column 4 lines 32-35: the decryption key is prestored in the decipherer). Both encipherer and decipherer are in the tuner apparatus or the receiving system.

As per claim 10, Tsukamoto further teaches a data recording/reproducing system in accordance with claim 8, wherein said public key and said secret key are keys inherent in the device model of said tuner (Tsukamoto: column 4 lines 12-15: the encryption key is prestored in encipherer; column 4 lines 32-35: the decryption key is prestored in the decipherer). Encipherer and decipherer are device models of tuner apparatus.

As per claim 15, Tsukamoto further teaches a data recording/reproducing system in accordance with claim 8, wherein said key encrypting means is provided for said tuner apparatus or said recording apparatus (Tsukamoto: column 4 lines 4-8: encipherer is coupled to descrambler; column 3 line 62: descrambler is coupled to tuner; Figure 2: the encipherer is

located between tuner and VTR apparatus). The encipherer can be provided for said tuner apparatus or said VTR apparatus.

As per claim 17, Tsukamoto further teaches Tsukamoto further teaches a data recording/reproducing system in accordance with claim 7, wherein said public key and said secret key are keys inherent in said VTR apparatus (Tsukamoto: column 4 lines 12-15: the encryption key is prestored in encipherer; column 4 lines 32-35: the decryption key is prestored in the decipherer), and said key encrypting means and said key decrypting means are provided for said VTR apparatus (Tsukamoto: Figure 2: the encipherer and decipherer are within the receiving system). The receiving system can be described as the VTR apparatus for which a recording/reproducing medium is included in the system along with several other components. Therefore, the key encrypting means and key decrypting means are provided for said VTR apparatus.

5. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori and further in view of Fox as applied to claim 8 above, and further in view of Matsumoto et al. U.S. Pat. No. 6345263 (hereinafter Matsumoto).

As per claim 11, Tsukamoto-Kori-Fox teaches a data recording/reproducing system in accordance with claim 8, Tsukamoto-Kori-Fox does not explicitly teach the use of a card reading means. However, Matsumoto teaches a data recording/reproducing system in accordance with claim 8, wherein said tuner apparatus has a card reading means capable of reading information recorded on an IC card (Matsumoto: column 2 line 9-12: IC card reader; Matsumoto: Figure 1: the IC card is inserted into the tuner apparatus). It would have been obvious to one having

ordinary skill in the art to establish a slot to insert IC card into the tuner apparatus for which the tuner apparatus contains IC card reading/writing apparatus to access the information stored in the IC card. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Tsukamoto, Kori, Fox, and Matsumoto because the IC card allows the tuner apparatus to decide whether the user has satisfy predetermined condition for recording/reproducing the digital data.

As per claim 12, Tsukamoto-Kori-Fox-Matsumoto teaches a data recording/reproducing system in accordance with claim 11. Matsumoto further teaches said public key and said secret key are keys inherent in the user ID recorded on said IC card (Matsumoto: column 7 lines 58-63:encryption key is stored in the IC card). The encryption key taught by Matsumoto is used for encryption of the information stored in the IC card. However, it would have been obvious to one having ordinary skill in the art to use the encryption key to encrypt the digital data stored within the system to prevent illegal recording/reproducing. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Tsukamoto, Kori, Fox, and Matsumoto because the encryption key stored in the IC card allows the encryption key to be stored in a portable medium instead of the tuner apparatus which has higher chance of being attacked.

As per claim 13, Tsukamoto-Kori-Fox-Matsumoto teaches a data recording/reproducing system in accordance with claim 11. Matsumoto further teaches said public key and said secret key are keys inherent in the service recorded on said IC card (Matsumoto: column 3 lines 7-11: the pay TV broadcasting system stores encryption key information). The encryption key

information stored by the service is used to encrypt the data transmitting to the receiver. Same rationale is applied here for combination as applied in claim 12.

6. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori and in view of Fox and in view of Matsumoto as applied to claim 12 above, and further in view of Masada U.S. Pat. No. 4928001 (hereinafter Masada).

As per claim 14, Tsukamoto-Kori-Fox-Matsumoto teaches a data recording/reproducing system in accordance with claim 12. Tsukamoto-Kori-Fox-Matsumoto uses the public key inherent in the IC card to carry out said second encrypting. Tsukamoto-Kori-Fox-Matsumoto does not explicitly teach the method of including at least another user ID on the IC card for carrying out said second encrypting for additional encrypted contents key. However, Masada teaches that limitation by teaching an IC card that includes multiple IDs (Masada: abstract and summary: to provide a memory medium which may be shared by a plurality of parties by dividing the memory medium into a plurality of discrete portions each of which may be accessed only by means of a predetermined different identification code). Therefore, it would have been obvious to one having ordinary skill in the art to include public keys and secret keys disclosed by Matsumoto within the IC card disclosed by Masada to carry out said second encrypting because it creates more encrypted contents key so that the system can switch the keys periodically with ease.

7. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori and in view of Fox as applied to claim 15 above, and further in view of Ishiguro.

As per claim 16, Tsukamoto-Kori-Fox teaches a data recording/reproducing system in accordance with claim 15.Tsukamoto-Kori-Fox does not explicitly the method of using common key to encrypt and decrypt said contents key. However, Ishiguro discloses a method of using common-key cryptography (Ishiguro: column 1 lines 30-32: in the common key cryptosystem, encryption key used upon encryption is the same as a key used upon decryption). Therefore, it would have been obvious to one having ordinary skill in the art to encrypt the contents key in the tuner apparatus with the common key and then allow the recording apparatus to decrypt the encrypted contents key using the common key if permitted because it allows the system to efficiently and rapidly change the key-encrypting key if desired.

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori and in view of Fox as applied to claim 17 above, and further in view of Ishiguro, and further in view of Komuro et al. U.S. Pat. No. 6223285 (hereinafter Komuro).

As per claim 18, Tsukamoto-Kori-Fox teaches a recording/reproducing system in accordance with claim 17. Tsukamoto-Kori-Fox does not explicitly the method of using common key to encrypt and decrypt said contents key. However, Ishiguro discloses a method of using common-key cryptography (Ishiguro: column 1 lines 30-32: in the common key cryptosystem, encryption key used upon encryption is the same as a key used upon decryption). Therefore, it would have been obvious to one having ordinary skill in the art to encrypt the contents key in the tuner apparatus with the common key and then allow the VTR apparatus to decrypt the encrypted contents key using the common key if permitted because it allows the system to efficiently and rapidly change the key-encrypting key if desired.

Furthermore, Tsukamoto-Kori-Fox-Ishiguro does not explicitly including multiple encryption and decryption means. However, Komuro teaches two encryption and decryption units (Komuro: figure 5A). Therefore, it would have been obvious to one having ordinary skill in the art to increase the number of encryption/decryption means to perform the common key cryptography disclosed by Ishiguro because multiple unit common key cryptosystem increase the security of the system by employing several rounds of encryption between encryption and decryption means.

9. Claims 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori as applied to claim 6 above, and further in view of Matsumoto et al. U.S. Pat. No. 5218638 (hereinafter Matsumoto2).

As per claim 19, Tsukamoto-Kori teaches a data recording/ reproducing system in accordance with claim 6. Tsukamoto further teaches the said key encrypting means and said key decrypting means are provided for said tuner apparatus (Tsukamoto: Figure 2: the decipherer is included in the receiving system; column 4 lines 4-8: encipherer is coupled to descrambler; column 3 line 62: descrambler is coupled to tuner; Figure 2: the encipherer is located between tuner and VTR apparatus). The receiving system can be described as the tuner apparatus for which a tuner is included in the system along with several other components.

Tsukamoto-Kori does not explicitly teach said second encrypting and said decrypting of said encrypted contents key are executed by using a common key, and said key encrypting means and said key decrypting means are provided for said tuner apparatus. However, Matsumoto2 teaches the use of common key to encrypt and decrypt information (Matsumoto2: column 12

lines 19-42: the common key is used to encipher and decipher service information). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Tsukamoto-Kori, and Matsumoto2 because the use of common key to encrypt the contents key would reduce the processing time and reduce the burden of the system y involving simpler computations.

As per claim 20, Tsukamoto-Kori-Matsumoto2 teaches a data recording/reproducing system in accordance with claim 19. Matsumoto2 further teaches said common key is inherent in said tuner apparatus or the device model of said tuner apparatus (Tsukamoto: column 4 lines 12-15: the encryption key is prestored in encipherer; column 4 lines 32-35: the decryption key is prestored in the decipherer). Both encipherer and decipherer are in the tuner apparatus or the receiving system.

As per claim 21, Tsukamoto-Kori-Matsumoto2 teaches a data recording/reproducing system in accordance with claim 19. Matsumoto2 further teaches said tuner apparatus has a card reading means capable of reading information recorded on an IC card, and said common key is inherent in the user ID recorded on said IC card or the service recorded on said IC card (Matsumoto2: column 12 lines43-53: the use of IC card; figure 13: ID-based key generating method; figure 7: IC card reader/writer). It would have been obvious to one having ordinary skill in the art to install the IC card reader/writer in the tuner apparatus for reading the information stored in an IC card and generate a common key based on the IDs stored in the card. Same rationale applies here as above in rejecting claim 19.

10. Claim 27 rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori as applied to claim 22 above, and further in view of Matsumoto.

As per claim 27, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 22. Tsukamoto-Kori does not explicitly teach the use of IC card to store billing information. However, Matsumoto teaches a system that stores the billing information on an IC card (Matsumoto: column 2 lines 9-10; column 2 lines 21-25: electronic money is subtracted from the IC card and stored in the information storage means). The use of IC card in a broadcasting tuner apparatus is well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Tsukamoto, Kori, and Matsumoto because IC card gives the system certain independent decision-making ability.

11. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori as applied to claim 4 above, and further in view of Ishiguro et al. U.S. Pat. No.5917910 (hereinafter Ishiguro).

As per claim 30, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. However, Tsukamoto-Kori does not explicitly teach the information regarding the inherence of said key subjected to said second encrypting is stored on said recording medium. Ishiguro teaches that limitation (Ishiguro: abstract: an encryption key based on inherent information inherent in a recording medium is generated; column 1 line 65- column 2 line 14). It would have been obvious to one having ordinary skill in the art to store the

encrypting key on a recording medium because it prohibits the file used for generating the encryption key to be duplicated with ease.

12. Claims 31-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori as applied to claim 4 above, and further in view of Schultz U.S. Pat. No. 6157723 (hereinafter Schultz).

As per claim 31, Tsukamoto-Kori teaches a data recording/reproducing system in accordance with claim 4. Tsukamoto-Kori does not explicitly disclose a method of switching the contents key at regular or irregular intervals. However, Schultz teaches a method of switching the contents keys at regular intervals (Schultz: column 1 lines 17-19: it is common to periodically change the encryption keys). Since the contents key is encryption key which is used to encrypt a data or file, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Tsukamoto, Kori, and Schultz because it is common to periodically change the encryption keys to enhance the security of the system and to maintain the integrity of the system.

As per claim 32 and 33, Tsukamoto-Kori-Schultz teaches a recording/reproducing system in accordance with claim 31. Tsukamoto teaches the method of writing encryption key in a predetermined portion of the data (Tsukamoto: figure 11). Tsukamoto does not explicitly teach the method of periodically switching the encryption key. However, Schultz teaches that limitation (Schultz: column 1 lines 13-14: it is common to periodically change the encryption keys). Therefore, it would have been obvious to one having ordinary skill in the art to overwrite

the old encryption key with the new encryption key in the predetermined portion of the data because it saves space and memory of the system.

As per claim 34, Tsukamoto-Kori-Schultz teaches a recording/reproducing system in accordance with claim 31. Tsukamoto-Kori-Schultz further teaches the tuner apparatus carries out said switching. Tsukamoto teaches the method of tuner apparatus receiving the encryption key (Tsukamoto: column 4 lines 12-15: encryption key included in the video signal is supplied by broadcasting station) and Schultz teaches the method of changing encryption keys periodically. Therefore, it would have been obvious to one having ordinary skill in the art to employ the tuner apparatus to switch the encryption key when broadcasting station transmits new encryption key. Same rationale applies here as above in rejecting claim 3.

As per claim 35, Tsukamoto-Kori-Schultz teaches a data recording/reproducing system in accordance with claim 31. Tsukamoto further teaches a receiving system in which the receiving system includes a clock to synchronized the operation of encryption and decryption (Tsukamoto: column 6 lines 8-25: supplies a time reference signal and date reference signal to clock upon receiving video program transmission; column 4 lines 50-56: clock synchronizes its operation therewith). The clock taught by Tsukamoto keeps track of date/time information. Therefore, it would have been obvious to one having ordinary skill in the art to use the clock to determine the reproduction timing of said encrypted contents key in response to said switching.

As per claim 36, Tsukamoto-Kori-Schultz teaches a data recording/reproducing system in accordance with claim 31. Kori further teaches the said encrypted digital data and said encrypted contents key are recorded at the recording position corresponding to said reproduction timing on said recording medium (Kori: figure 11 and paragraph 79: the data portion of the A/V data;

paragraph 90: stores the A/V data file to a predetermined region). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to record the encrypted contents key and encrypted digital data at the time of recording because it allows the system to determine the condition for which reproduction is allowed by checking the encrypted contents key along with other information.

As per claim 37, Tsukamoto-Kori-Schultz teaches a recording/reproducing system in accordance with claim 36. Tsukamoto further teaches an access control unit receives a date/time reference when a video signal is transmitted from the broadcasting station (Tsukamoto: column 4 lines 50-57: receives a time reference signal and a date reference signal). It would have been obvious to one having ordinary skill in the art to switch the encryption key when it is transmitted from the broadcasting station (Tsukamoto: column 4 lines 12-17: the encryption key is in the access control signal supplied by broadcasting station).

Tsukamoto does not explicitly teach the method of recording switch timing on said recording medium. However, Kori further teaches that limitation (Kori: paragraph 79-82 and figure 12). It would have been obvious to include the switch timing into the digital data to keep track of the time of encryption. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it allows the system to have knowledge on when the encryption/decryption should take place.

As per claim 38, Tsukamoto-Kori-Schultz teaches a recording/reproducing system in accordance with claim 31. Tsukamoto further teaches the method of outputting the contents key or encrypted contents key before outputting said encrypted digital data corresponding to said contents key for use after switching (Tsukamoto: column 4 lines 4-18: encipherer encrypts

according to an encryption key...encryption key is supplied by access controller or included in the video signals; column 4 line 4: encipherer is coupled to descrambler; column 3 line 62: descrambler is coupled to tuner; column 11 lines 28-34: recording/reproducing section records on storage medium in storage cassette video signals supplied by access controller; column 11 lines 48-52: encryption key is stored in and read from storage medium). It implies that the contents key has been outputted for use by the recording/reproducing section before encrypting the digital data by the encipherer, which is coupled to the tuner apparatus.

13. Claims 39-45, 47-49, 53-57, 59, 63-65, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsukamoto in view of Kori and further in view of Aizawa.

As per claim 39, Tsukamoto teaches a recording apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data (Tsukamoto: column 4 lines 4-18: encrypt the video signal...encryption key is prestored in encipherer or supplied by broadcasting station), a storing means for storing key-encrypting key (Tsukamoto: column 5 lines 17-19: access controller stores both access-control signals and the encryption keys), a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key (Tsukamoto: column 5 lines 5-19: as a function of the signals supplied to access controller by clock, user interface, etc. access controller stores both

access-control signal and the encryption keys; column 7 lines 50-51: access control signal indicating that reproduction is allowed until date Y; column 7 lines 66-67: access-control signal indicating that reproduction is allowed until time T; the clock generate the date/time signal for which a recording/reproducing medium can record/reproduce the data file implies there is a starting time to keep track of the interval), and a recording medium for receiving said encrypted digital data (Tsukamoto: column 4 lines 19-21: records on storage medium video signals supplied by encipherer).

Tsukamoto does not explicitly teach a key-encrypting key generating means for generating a key-encrypting key for subjecting said contents key to second encrypting. However, Kori teaches that limitation (Kori: paragraph 81: the user management key ku is supplied from the A/V data supplying side to each user; paragraph 80: with a user management key ku... data encrypting key kd are encrypted). The key-encrypting key can be generated by the A/V data supplying side and transmit to users for double encryption. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teaching of Kori within the system of Tsukamoto because with the user management key ku, it allows the data transmission side to restrict the users from using the data file and is suitable for A/V data files that are quantitatively created.

Furthermore, Tsukamoto does not explicitly teach a key encrypting means for generating an encrypted contents key by subjecting said contents key to said second encrypting by using said key-encrypting key. However, Kori further teaches that limitation (paragraph 80: with a user management key ku...data encrypting key kd are encrypted). It would have been obvious to one having ordinary skill in the art to perform the second encryption within the encipherer, which is

taught by Tsukamoto. It also would have been obvious to create a secondary encipherer within the system to perform second encrypting. Same rationale applies here as in previous paragraph.

Furthermore, Tsukamoto teaches the method of erasing the video program on a certain date wherein the predetermined condition is satisfied if the key-encrypting key was stored on a previous date that is less than a specific number of days from a current date, or if a number of reproductions of the digital data is less than a specific number of reproduction (Tsukamoto: column 9 lines 1-18 and column 9 line 64 – column 10 line 8). Tsukamoto does not explicitly teach the method of only deleting the key-encrypting key if key-encrypting key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the key-encrypting key at the time the A/V data is transmitted (Kori: [0081] and [0083]: transmitting the user management key to restrict the user to use the A/V data). Although Kori does not explicitly disclose only deleting the decryption key to render the content useless, Aizawa discloses deleting only the content encryption key to prohibit decryption of data (Aizawa: column 5 lines 46-55). It would have been obvious to one having ordinary skill in the art to erase only the key-encrypting key because the user management key ku is used is used to restrict access to the programming and by deleting the user management key, the encrypted video programming is rendered useless. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it restricts the user to use the A/V data without the presence of the user management key.

Furthermore, Tsukamoto teaches a recording medium for receiving said encrypted digital data on a predetermined recording medium. Tsukamoto does not explicitly teach the method of recording encrypted contents key and all or part of said relationship information and encrypted

digital data for recording. However, Kori further teaches that limitation (Kori: paragraph 79-82 and figure 12). It would have been obvious to include the relationship information of the digital data encryption and contents key encryption information into the digital data to keep track of the time of encryption. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it allows the system to have knowledge on when the encryption/decryption should take place.

As per claim 40, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39. Tsukamoto further teaches said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored (Tsukamoto: column 9 lines 1-9: one access-control signal indicate that the video programming is to be erased on a certain date Y). According to Kori in claim 39, the A/V data supplier supplies the key-encrypting key. By erasing the video programming, the key-encrypting key should be erased as well.

As per claim 41, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39or 40. Tsukamoto further teaches said relationship-information is information-related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said key-encrypting key generating means generates said key-encrypting key, a date/time when said storing means stores said key encrypting key, a date/time when said key encrypting means encrypts said contents key by using said key-encrypting key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium (Tsukamoto: column 6 lines 8-25: supplies a time reference signal and date reference signal to clock upon receiving video program transmission; column 4 lines 50-56: clock synchronizes its

operation therewith). The clock taught by Tsukamoto keeps track of date/time information. Therefore, it would have been obvious to one having ordinary skill in the art to assume the purpose of generating the relationship information is to synchronize the operation within the system. By using the clock, it synchronizes the operation within the recording apparatus.

As per claim 42, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39. Tsukamoto further teaches said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined of times (Tsukamoto: column 7 lines 19-38: the video program can be reproduced up to N times). Since the decryption of the digital data requires key-encrypting key supplied by the broadcasting station. It would have been obvious to delete the digital program or the key-encrypting key if the digital data has been reproduced for more than the predetermined number of times.

As per claim 43, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39. Tsukamoto further teaches a contents key generating means for generating said contents key is provided, and said contents key encrypting means receives said contents key from said contents key generating means (Tsukamoto: column 4 lines 12-18: the encryption key is supplied by access controller, or included in the in the video signals supplied by the broadcasting station; column 4 lines 5-19: the access controller receives signals through clock, modem, user interface, etc.... access controller controls the operation of encipherer and decipherer). It would have been obvious to one having ordinary skill in the art to assume by receiving a contents key from a broadcasting means, there exists a contents key generating means that generates a contents key from the broadcasting station. On the other hand, Tsukamoto does not explicitly teach the

method of using encipherer to encrypt the contents key. However, it would have been obvious to one having ordinary skill in the art to use the encipherer or another encipherer to encrypt the contents key.

As per claim 44, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39. Tsukamoto further teaches said contents encrypting means receives said contents key from a broadcasting station and uses said contents key (Tsukamoto: column 4 lines 12-18: the encryption key is supplied by access controller, or included in the in the video signals supplied by the broadcasting station; column 4 lines 5-19: the access controller receives signals through clock, modem, user interface, etc.... access controller controls the operation of encipherer and decipherer).

As per claim 45, Tsukamoto-Kori in accordance with claim 39 teaches a reproducing apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising: key-encrypting key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with claim 39 (Tsukamoto: column 11 lines 28-44: Recording/reproducing section records video signals supplied by access controller in on storage medium in storage cassette and also reads previously recorded video signals and previously recorded access-control signals from the storage medium; column 5 lines 40-53: storage medium contains access condition memory; column 5 lines 18-19: access condition memory stores encryption key), for specifying a key-encrypting key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information (Tsukamoto: column 7 lines 20-38: right to reproduce a video program for N times; column 7 line50-51: indicating reproduction is

allowed until date Y; column 7 lines 66-67: reproduction is allowed until time T), and for retrieving and obtaining said key encrypting key from said storing means of said recording means (Tsukamoto: recording/reproducing section recovers video signals from storage medium; column 5 lines 40-54: storage medium contains access condition memory; column 5 lines 18-19: encryption keys are stored in access condition memory), key decrypting means for receiving said encrypted contents key corresponding to said encrypted digital data to be reproduced, from said predetermined recording medium (Tsukamoto: column 4 lines 29-40: Decipherer decrypts according to an encryption key; encryption key is stored in storage medium), for receiving said key-encrypting key, and for decrypting said encrypted contents key by using said key-encrypting key, and a contents decrypting means for decrypting said encrypted digital data by using said contents key from said key decrypting means (Kori: page 5 paragraph 82: decrypt the key kd and then use kd to decrypt the A/V data). Same rationale applies here as above in rejecting claim 39.

As per claim 47, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39. Tsukamoto further said relationship-information is information-related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said key-encrypting key generating means generates said key-encrypting key, a date/time when said storing means stores said key encrypting key, a date/time when said key encrypting means encrypts said contents key by using said key-encrypting key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium (Tsukamoto: column 6 lines 8-25: supplies a time reference signal and date reference signal to clock upon

receiving video program transmission; column 4 lines 50-56: clock synchronizes its operation therewith). Same rationale applies here as above in rejecting claim 41.

As per claim 48, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 47. Tsukamoto further teaches a contents key generating means for generating said contents key is provided, and said contents key encrypting means receives said contents key from said contents key generating means (Tsukamoto: column 4 lines 12-18: the encryption key is supplied by access controller, or included in the in the video signals supplied by the broadcasting station; column 4 lines 5-19: the access controller receives signals through clock, modem, user interface, etc.... access controller controls the operation of encipherer and decipherer). Same rationale applies here as above in rejecting claim 43.

As per claim 49, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 47. Tsukamoto further teaches said contents encrypting means receives said contents key from a broadcasting station and uses said contents key (Tsukamoto: column 4 lines 12-18: the encryption key is supplied by access controller, or included in the in the video signals supplied by the broadcasting station; column 4 lines 5-19: the access controller receives signals through clock, modem, user interface, etc.... access controller controls the operation of encipherer and decipherer).

As per claim 53, Tsukamoto teaches a recording apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising a contents key generating means for generating a contents key for encrypting digital data (Tsukamoto: column 4 lines 4-18: encrypt the video signal...encryption key is prestored in encipherer or supplied by broadcasting station), a storing

means for storing said contents key generated by said contents key generating means (Tsukamoto: column 5 lines 17-19: access controller stores both access-control signals and the encryption keys), a contents encrypting means for encrypting said digital data by using said contents key (Tsukamoto: column 4 lines 4-9: encipherer is coupled to descrambler to encrypt descrambled video signals according to an encryption key), and a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said contents key (Tsukamoto: column 5 lines 5-19: as a function of the signals supplied to access controller by clock, user interface, etc. access controller stores both access-control signal and the encryption keys; column 7 lines 50-51: access control signal indicating that reproduction is allowed until date Y; column 7 lines 66-67: access-control signal indicating that reproduction is allowed until time T; the clock generate the date/time signal for which a recording/reproducing medium can record/reproduce the data file implies there is a starting time to keep track of the interval), and a recording means for receiving said encrypted digital data (Tsukamoto: column 4 lines 19-21: records on storage medium video signals supplied by encipherer).

Furthermore, Tsukamoto teaches the method of erasing the video program on a certain date and predetermined condition is satisfied if the key-encrypting key was stored on a previous date that is less than a specific number of days from a current date, or if a number of reproductions of the digital data is less than specific number of reproduction (Tsukamoto: column 9 lines 1-18 and column 9 line 64 – column 10 line 27). Tsukamoto does not explicitly teach the method of deleting the key-encrypting key if key-encrypting key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the

key-encrypting key at the time the A/V data is transmitted. Although Kori does not explicitly disclose only deleting the decryption key to render the content useless, Aizawa discloses deleting only the content encryption key to prohibit decryption of data (Aizawa: column 5 lines 46-55). It would have been obvious to one having ordinary skill in the art to erase the key-encrypting key at the time video programming is erased. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it saves memory of the system and it maintains the security of the system by periodically changing the key-encrypting key.

Furthermore, Tsukamoto teaches a recording medium for receiving said encrypted digital data on a predetermined recording medium. Tsukamoto does not explicitly teach the method of recording encrypted contents key and all or part of said relationship information and encrypted digital data for recording. However, Kori further teaches that limitation (Kori: paragraph 79-82 and figure 12). It would have been obvious to include the relationship information of the digital data encryption and contents key encryption information into the digital data to keep track of the time of encryption. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it allows the system to have knowledge on when the encryption/decryption should take place.

As per claim 54, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 53. Tsukamoto further teaches said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored in said storing means of said recording apparatus in accordance with claim 46 (Tsukamoto: column 9 lines 1-9: one access-control signal indicate that the video programming is to be erased on a certain date Y). According to Kori in claim 53, the A/V data supplier supplies the key-encrypting key (Kori: paragraph 81: the

user management key ku is supplied from the A/V data supplying side to each user). By erasing the video programming, the key-encrypting key should be erased as well.

As per claim 55, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 53 or 54. Tsukamoto further teaches said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said contents key generating means generates said contents key, a date/time when said storing means stores said contents key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium (Tsukamoto: column 6 lines 8-25: supplies a time reference signal and date reference signal to clock upon receiving video program transmission; column 4 lines 50-56: clock synchronizes its operation therewith). The clock taught by Tsukamoto keeps track of date/time information. Therefore, it would have been obvious to one having ordinary skill in the art to assume the purpose of generating the relationship information is to synchronize the operation within the system. By using the clock, it synchronizes the operation within the recording apparatus.

As per claim 56, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 53. Tsukamoto further teaches said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined of times (Tsukamoto: column 7 lines 19-38: the video program can be reproduced up to N times). Since the decryption of the digital data requires key-encrypting key supplied by the broadcasting station. It would have been obvious to delete the digital program or the key-

encrypting key if the digital data has been reproduced for more than the predetermined number of times.

As per claim 57, Tsukamoto-Kori in accordance with claim 53 teaches a reproducing apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising: a contents key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with claim 53 (Tsukamoto: column 11 lines 28-44: Recording/reproducing section records video signals supplied by access controller in on storage medium in storage cassette and also reads previously recorded video signals and previously recorded access-control signals from the storage medium; column 5 lines 40-53: storage medium contains access condition memory; column 5 lines 18-19: access condition memory stores encryption key), for specifying a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information (Tsukamoto: column 7 lines 20-38: right to reproduce a video program for N times; column 7 line50-51: indicating reproduction is allowed until date Y; column 7 lines 66-67: reproduction is allowed until time T), and for retrieving and obtaining said contents key from said storing means of said recording means (Tsukamoto: recording/reproducing section recovers video signals from storage medium; column 5 lines 40-54: storage medium contains access condition memory; column 5 lines 18-19: encryption keys are stored in access condition memory), and a contents decrypting means for decrypting said encrypted digital data by using said contents key from said key decrypting means (Kori: page 5 paragraph 82: decrypt the key kd and then use kd to decrypt the A/V data). Same rationale applies here as above in rejecting claim 39.

As per claim 59, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 53. Tsukamoto further teaches said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said contents key generating means generates said contents key, a date/time when said storing means stores said contents key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium (Tsukamoto: column 6 lines 8-25: supplies a time reference signal and date reference signal to clock upon receiving video program transmission; column 4 lines 50-56: clock synchronizes its operation therewith). The clock taught by Tsukamoto keeps track of date/time information. Therefore, it would have been obvious to one having ordinary skill in the art to assume the purpose of generating the relationship information is to synchronize the operation within the system. By using the clock, it synchronizes the operation within the recording apparatus.

As per claim 60, Tsukamoto-Kori in accordance with claim 58 teaches a reproducing apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising: a contents key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with one of claims 58 or 59 (Tsukamoto: column 11 lines 28-44: Recording/reproducing section records video signals supplied by access controller in on storage medium in storage cassette and also reads previously recorded video signals and previously recorded access-control signals from the storage medium; column 5 lines 40-53: storage medium contains access condition memory; column 5 lines 18-19: access condition memory stores

encryption key), for specifying a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information (Tsukamoto: column 7 lines 20-38: right to reproduce a video program for N times; column 7 line50-51: indicating reproduction is allowed until date Y; column 7 lines 66-67: reproduction is allowed until time T), and a contents decrypting means for decrypting said encrypted digital data by using said contents key (Kori: page 5 paragraph 82: decrypt the key kd and then use kd to decrypt the A/V data). Same rationale applies here as above in rejecting claim 39.

Tsukamoto teaches a recording medium for receiving said encrypted digital data on a predetermined recording medium. Tsukamoto does not explicitly teach the method of taking out the contents key if contents key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the contents key at the time the A/V data is transmitted. It would have been obvious to one having ordinary skill in the art to erase the contents key at the time video programming is erased. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it saves memory of the system and it maintains the security of the system by periodically changing the contents key.

As per claim 61, Tsukamoto-Kori teaches a reproducing apparatus in accordance with claim 60. Tsukamoto further teaches said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored in said storing means of said recording apparatus (Tsukamoto: column 9 lines 1-9: one access-control signal indicate that the video programming is to be erased on a certain date Y). According to Kori in claim 60, the A/V data supplier supplies the key-encrypting key (Kori: paragraph 81: the user management

key ku is supplied from the A/V data supplying side to each user). By erasing the video programming, the key-encrypting key should be erased as well.

As per claim 62, Tsukamoto-Kori teaches a reproducing apparatus in accordance with claim 60. Tsukamoto further teaches said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined of times (Tsukamoto: column 7 lines 19-38: the video program can be reproduced up to N times). Since the decryption of the digital data requires contents key supplied by the broadcasting station. It would have been obvious to delete the digital program or the contents key if the digital data has been reproduced for more than the predetermined number of times.

As per claim 63, Tsukamoto-Kori teaches a recording apparatus in accordance with claim 39 or 53. Tsukamoto further teaches a recording apparatus provided with a billing means for charging the amount of billing for recording said data at the time when said recording means records said encrypted digital data on said predetermined recording medium (Tsukamoto: column 6 lines 27-46: the user can pay to get full access to record or reproduce a video program; column 6 lines 60-64: the recorded video can be reproduced upon payment; figure 7a: the signal sent from the access control include purchase information). The signal sent from the access control implies that the billing information has been stored and generated within the tuner apparatus.

As per claim 64, Tsukamoto further teaches a recording apparatus in accordance with one of claims 39 or 53, wherein said predetermined recording medium is a video tape (Tsukamoto: column 4 lines 25-29: the storage medium is a video tape).

As per claim 65, Tsukamoto-Kori teaches a recording apparatus in accordance with one of claims 39 or 53. Kori further teaches the predetermined recording medium is a hard disk (Kori: paragraph 52: the file in the memory is stored on a recording medium such as a hard disc). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teaching of Kori within the system of Tsukamoto because it is well known in the art to record/download digital data on a computer thus it would require a hard disk to store the digital data.

As per claim 68, Tsukamoto teaches a recording apparatus (Tsukamoto: column 3 lines 48-49: a recording/reproducing section; column 4 lines 25-26: digital video tape recording/reproducing device) comprising a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data (Tsukamoto: column 4 lines 4-18: encrypt the video signal...encryption key is prestored in encipherer or supplied by broadcasting station), a storing means for storing key-encrypting key (Tsukamoto: column 5 lines 17-19: access controller stores both access-control signals and the encryption keys), a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key (Tsukamoto: column 5 lines 5-19: as a function of the signals supplied to access controller by clock, user interface, etc. access controller stores both access-control signal and the encryption keys; column 7 lines 50-51: access control signal indicating that reproduction is allowed until date Y; column 7 lines 66-67: access-control signal indicating that reproduction is allowed until time T; the clock generate the date/time signal for

which a recording/reproducing medium can record/reproduce the data file implies there is a starting time to keep track of the interval), and a recording medium for receiving said encrypted digital data (Tsukamoto: column 4 lines 19-21: records on storage medium video signals supplied by encipherer).

Tsukamoto does not explicitly teach a key-encrypting key generating means for generating a key-encrypting key for subjecting said contents key to second encrypting. However, Kori teaches that limitation (Kori: paragraph 81: the user management key ku is supplied from the A/V data supplying side to each user; paragraph 80: with a user management key ku... data encrypting key kd are encrypted). The key-encrypting key can be generated by the A/V data supplying side and transmit to users for double encryption. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teaching of Kori within the system of Tsukamoto because with the user management key ku, it allows the data transmission side to restrict the users from using the data file and is suitable for A/V data files that are quantitatively created.

Furthermore, Tsukamoto does not explicitly teach a key encrypting means for generating an encrypted contents key by subjecting said contents key to said second encrypting by using said key-encrypting key. However, Kori further teaches that limitation (paragraph 80: with a user management key ku...data encrypting key kd are encrypted). It would have been obvious to one having ordinary skill in the art to perform the second encryption within the encipherer, which is taught by Tsukamoto. It also would have been obvious to create a secondary encipherer within the system to perform second encrypting. Same rationale applies here as in previous paragraph.

Furthermore, Tsukamoto teaches the method of erasing the video program on a certain date wherein the predetermined condition is satisfied if the key-encrypting key was stored on a previous date that is less than a specific number of days from a current date, or if a number of reproductions of the digital data is less than a specific number of reproduction (Tsukamoto: column 9 lines 1-18 and column 9 line 64 – column 10 line 8). Tsukamoto does not explicitly teach the method of deleting the key-encrypting key if key-encrypting key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the key-encrypting key at the time the A/V data is transmitted. Although Kori as modified does not explicitly disclose only deleting the decryption key to render the content useless, Aizawa discloses deleting only the content encryption key to prohibit decryption of data (Aizawa: column 5 lines 46-55). It would have been obvious to one having ordinary skill in the art to erase the key-encrypting key at the time video programming is erased. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it saves memory of the system and it maintains the security of the system by periodically changing the key-encrypting key.

Furthermore, Tsukamoto teaches a recording medium for receiving said encrypted digital data on a predetermined recording medium. Tsukamoto does not explicitly teach the method of recording encrypted contents key and all or part of said relationship information and encrypted digital data for recording. However, Kori further teaches that limitation (Kori: paragraph 79-82 and figure 12). It would have been obvious to include the relationship information of the digital data encryption and contents key encryption information into the digital data to keep track of the time of encryption. Therefore, it would have been obvious to combine the teaching of Kori

within the system of Tsukamoto because it allows the system to have knowledge on when the encryption/decryption should take place.

Furthermore, Tsukamoto teaches a data recording/reproducing system comprising a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data (Tsukamoto: column 4 lines 4-9: encipherer is coupled to descrambler to encrypt descrambled video signals to produce encrypted video signals; column 3 line 62: descrambler is coupled to tuner; column 3 line 51: tuner receives input digital signals), a recording means for recording said encrypted digital data and said encrypted contents key on a recording medium, a reproducing means for reproducing said encrypted digital data from said recording medium (Tsukamoto: column 4 lines 19-25: records video signal from encrypting means), and a decrypting means for decrypting said encrypted digital data (Tsukamoto: column 4 lines 29-32: decrypt encrypted signals according to an encryption key). Tsukamoto does not explicitly teach key-encrypting key method for the encryption key and method for decrypting the encrypting key to decrypt the data. However, Kori teaches the method of encrypting contents key to generate an encrypted contents key to encrypt digital data (Kori: page 5 paragraph 79: A/V data is encrypted with key kd, and kd is encrypted corresponding to a predetermined key), and decrypting said encrypted contents key to restore said contents key, and a contents decrypting means for decrypting said encrypted digital data by using said contents key to obtain said digital data (Kori: page 5 paragraph 82: decrypt the key kd and then use kd to decrypt the A/V data), and wherein said encrypted contents key is recorded in a data area on said recording medium, from which data is not output outside (Kori:[0080]-[0081]: the data key is stored in header portion of the data). The key encrypting/decrypting method and contents

encrypting/decrypting method can be carried out by the decipherer and encipherer within Tsukamoto's system or it can be carried out by adding separate encrypting/decrypting means for encrypting/decrypting said contents key as well known in the art. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teaching of Kori within the system of Tsukamoto because using encrypted contents key would allow the system to be dual encrypted and it would take cryptanalysts more time and more a lot more effort to break the system if possible.

Furthermore, Tsukamoto teaches the method of erasing the video program on a certain date wherein the predetermined condition is satisfied if the key-encrypting key was stored on a previous date that is less than a specific number of days from a current date, or if a number of reproductions of the digital data is less than a specific number of reproduction (Tsukamoto: column 9 lines 1-18 and column 9 line 64 – column 10 line 8). Tsukamoto does not explicitly teach the method of deleting the key-encrypting key if key-encrypting key satisfies a predetermined condition. However, Kori teaches the method of A/V data supplier supplies the key-encrypting key at the time the A/V data is transmitted (Kori: [0081] and [0083]: transmitting the user management key to restrict the user to use the A/V data). It would have been obvious to one having ordinary skill in the art to erase only the key-encrypting key because the user management key ku is used is used to restrict access to the programming and by deleting the user management key, the encrypted video programming is rendered useless. Therefore, it would have been obvious to combine the teaching of Kori within the system of Tsukamoto because it restricts the user to use the A/V data without the presence of the user management key.

Response to Arguments

14. Applicant's arguments filed 1/6/06 have been fully considered but they are not persuasive.

Regarding the remarks, applicant argues that the reference do not disclose only deleting the key encrypting key. However, Kori discloses that the user management key (key-encrypting key) is used to restrict user to use the A/V data. Therefore, even if a user possesses the encrypted A/V data, without the user management key, the user will not be able to use the A/V data and it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to selectively erase the video program or the key-encrypting key while leaving encrypted digital data to prevent the user from access the A/V data. Furthermore, examiner has further applied Aizawa reference to more explicitly disclose this limitation (Aizawa: column 5 lines 46-55).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Davis U.S. Pat. No. 5825879 discloses an encrypted data content is transferred to a subscriber for storage and the subscriber is allowed access to the data only when payment has been paid to receive decryption key (Davis: column 3 lines 27-43).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC